Introduction to Cyber Security

Fundamentals of Web / Mobile Application Security

March 2021

Agenda

In today's session, you will learn about:

- Web Application Security
- Mobile Application Vulnerabilities
- Mobile Device Management

Source: Freepik

What is Web Application Security?

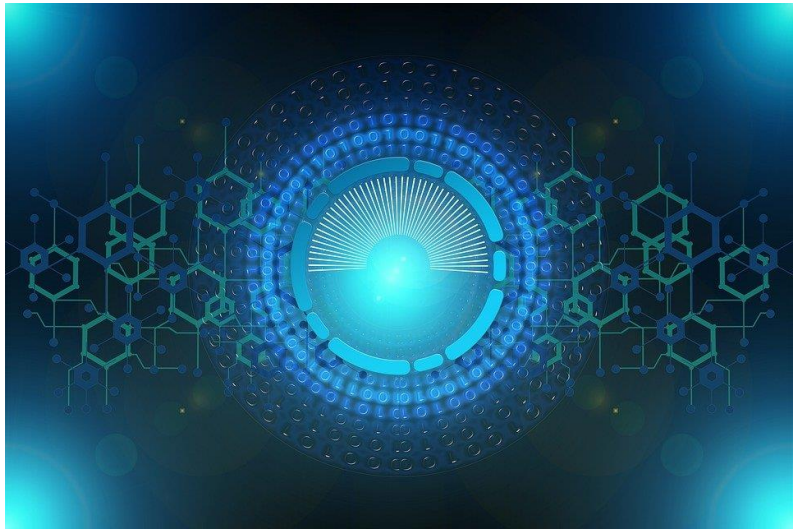
Created by fae frey
from Noun Project

Web application security is the process of protecting websites and online services against different security threats that exploit vulnerabilities in an application's code.

Web Application Security

The following is a Web Application Security Checklist:

- Error handling and logging
- Data Protection
- Configuration and Operations
- Authentication
- Session Management
- Input and Output Handling
- Access Control



Source: Pixabay

Name of the Activity

Behind the Door Number

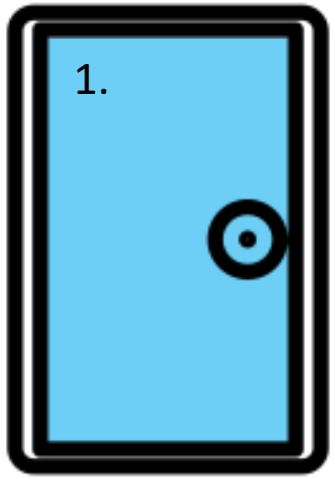
Instructions

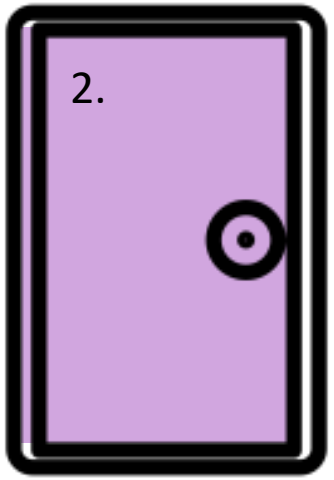
Mode: **In-session**

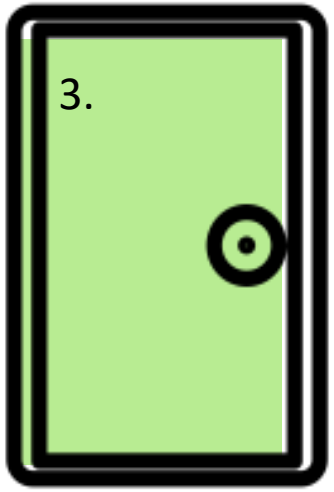
Duration: **5 minutes**

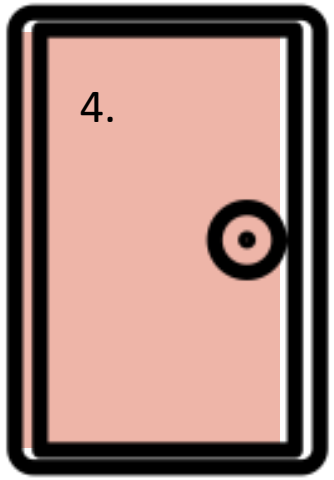
Materials Required: **None**

Knowledge Check – Behind the Door Number





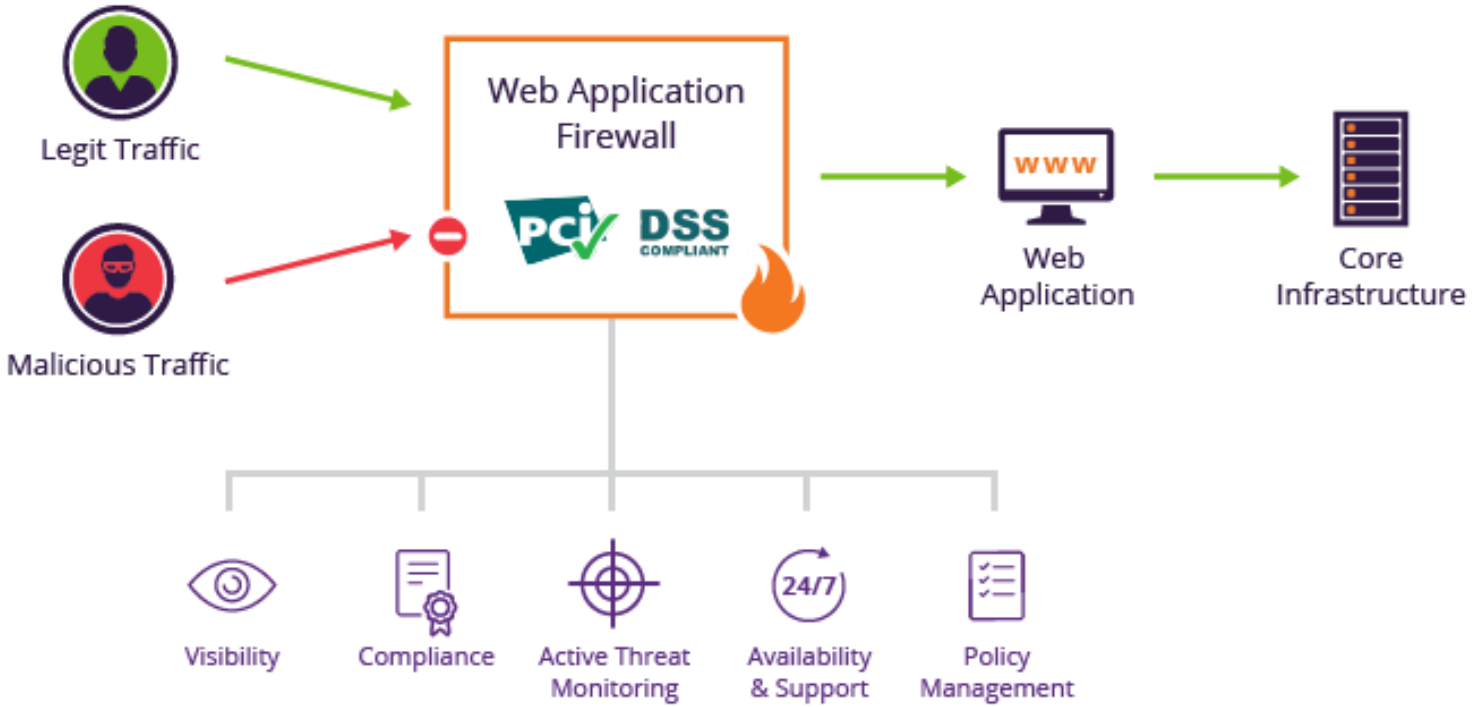




Source: Noun project

Securing the Web Server and Other Components

- Switch Off Unnecessary Functionality
- Limit and Secure Remote Access
- Use Accounts with Limited Privileges
- Permissions and Privileges
- Segregate Development, Testing and Live Environments
- Segregate Data
- Always Install Security Patches
- Monitor and Audit the Servers and Logs
- Use Security Tools



Why do perpetrators think web applications are high-priority targets?

Created by fae frey
from Noun Project

Securing the Web Server and Other Components

Perpetrators consider web applications high-priority targets due to:

- The inherent complexity
- High value rewards
- Ease of execution

Name of the Activity

Fill in the Blanks

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Common Weakness Enumeration

- The 2020 Common Weakness Enumeration (CWE™) Top 25 Most Dangerous Software Weaknesses (CWE Top 25) is a demonstrative list of the most common and impactful issues experienced over the previous two calendar years. These weaknesses are dangerous because they are often easy to find, exploit, and can allow adversaries to completely take over a system, steal data, or prevent an application from working.

Source: Freepik

The CWE Top 25

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44
[11]	CWE-190	Integer Overflow or Wraparound	15.81
[12]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13.67
[13]	CWE-476	NULL Pointer Dereference	8.35
[14]	CWE-287	Improper Authentication	8.17
[15]	CWE-434	Unrestricted Upload of File with Dangerous Type	7.38
[16]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.95
[17]	CWE-94	Improper Control of Generation of Code ('Code Injection')	6.53
[18]	CWE-522	Insufficiently Protected Credentials	5.49
[19]	CWE-611	Improper Restriction of XML External Entity Reference	5.33
[20]	CWE-798	Use of Hard-coded Credentials	5.19
[21]	CWE-502	Deserialization of Untrusted Data	4.93
[22]	CWE-269	Improper Privilege Management	4.87
[23]	CWE-400	Uncontrolled Resource Consumption	4.14
[24]	CWE-306	Missing Authentication for Critical Function	3.85
[25]	CWE-862	Missing Authorization	3.77

What is Mobile App Security?

Created by fae frey
from Noun Project

Mobile Application Security

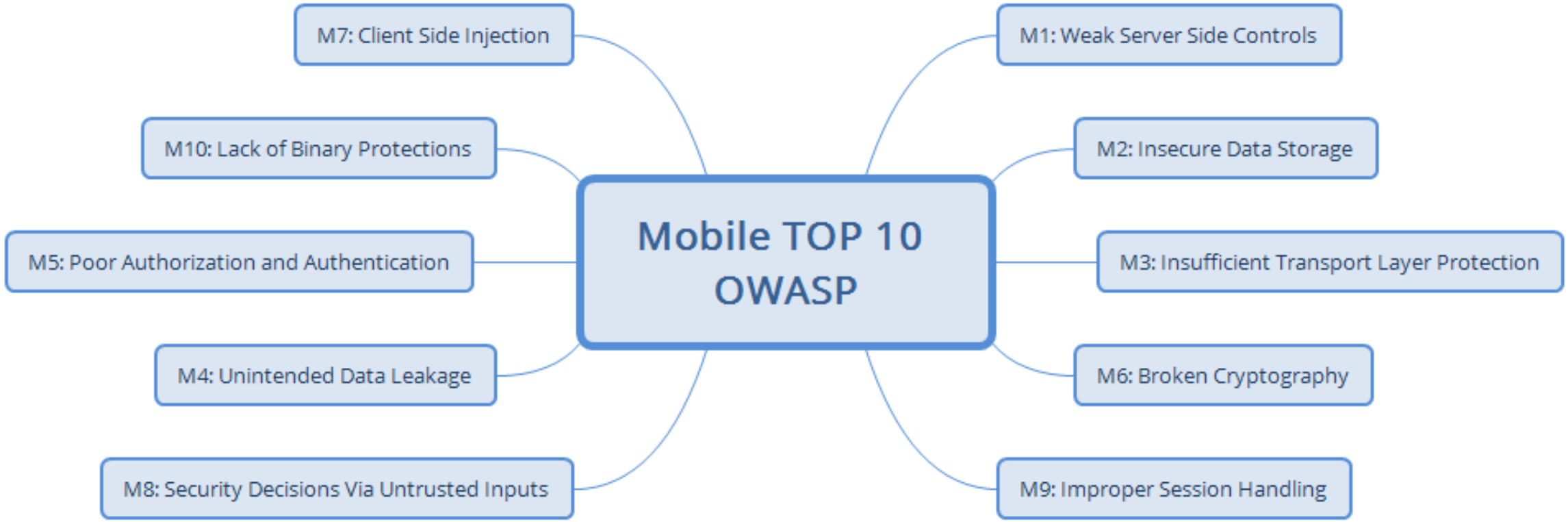
Mobile app security is the measure and means of defending mobile device apps from digital fraud in the form of malware, hacking, and other criminal manipulation.

Source: The Noun Project

When a mobile application is compromised by malware or a device user downloads an unauthorized rogue app that isn't actually officially launched, they stand a high risk of being a victim of digital fraud

Source: The Noun Project

Mobile Apps- Top 10 Risks



Mobile Apps- Top 10 Risks Countermeasures

Countermeasures:

- Do not root your phone.
- Do not download applications from untrusted third-party sources.
- Do not click on suspicious emails.
- Do not open suspicious SMS.
- Use strong passwords/patterns.

Mobile Application Security Best Practices

- Enact Digital Security Training
- Proactively Monitor for Rogue Apps
- Only Download from Trusted Sources
- Improve Data Security
- Avoid Saving Passwords
- Force User Session End
- Go Beyond Anti-Malware
- Invest in Mobile App Security Services

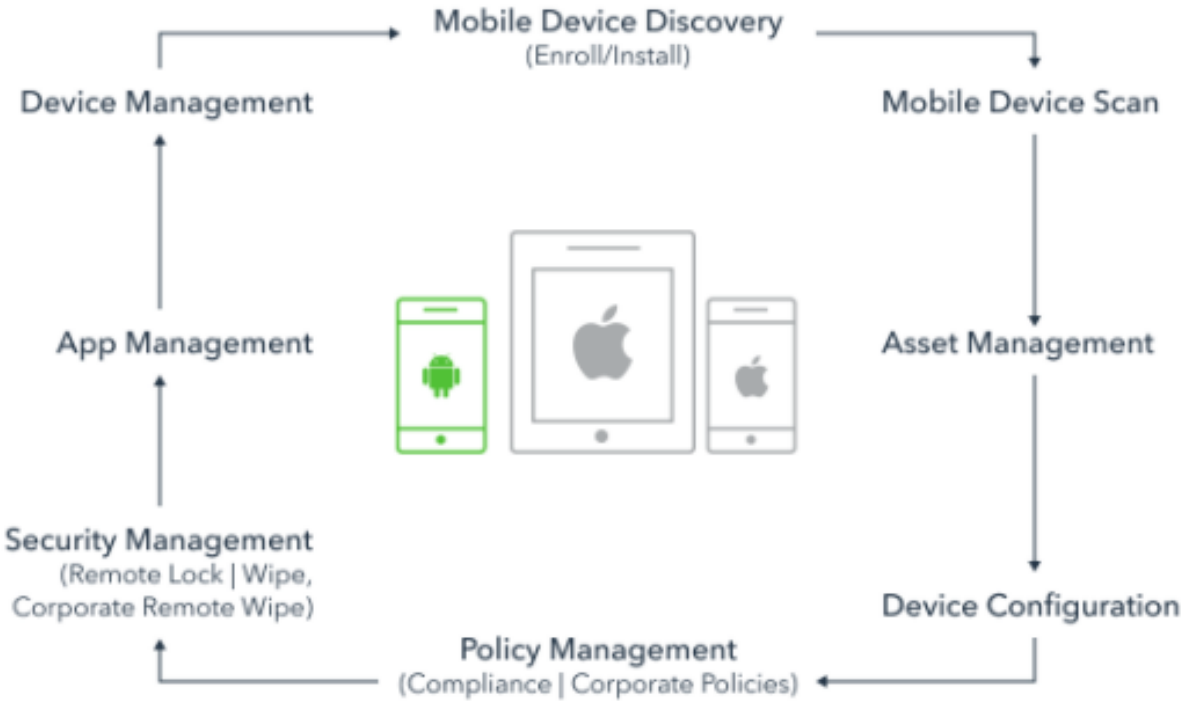
Source: Pixabay

What is Mobile Device Management?

Created by fae frey
from Noun Project

Mobile Device Management

MDM is the process of managing a mobile device through it's entire lifecycle in an enterprise. MDM solution enables administrators to optimize the functionality of mobile devices, including smartphones and tablets, while securing their enterprise from threats.



Mobile Device Management

An administrator has to:

- Come up with strong security policies.
- Use complex password policies.
- Install Updates to Antivirus software.
- Publish enterprise policy for the cloud.
- Specify session timeout through the gateway.

Source: The Noun Project

Name of the Activity

Face off

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Difference between
Mobile App Security
and
Mobile Device Management

Name of the Activity

Who am I?

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Who am I?

1. I am a measure and means of defending mobile device apps from digital fraud.

   Mobile Application Security

2. I am a type of counterfeit app designed to mimic trusted brands or apps with non-advertised malicious features.

   Rogue App

3. I am the process of protecting websites and online services against different security threats.

   Web Application Security

4. I am the process of managing a mobile device through it's entire lifecycle in an enterprise.

   Mobile Device Management

5. I secure all data transmissions.

   Cryptography

Summary

In this session, you learnt about:

- Web Application Security
- Mobile Application Vulnerabilities
- Mobile Device Management